BULL. AUSTRAL. MATH. SOC. 11R29, 11R21
VOL. 35 (1987) 231-245

EXPONENTS OF THE CLASS GROUPS OF IMAGINARY ABELIAN NUMBER FIELDS

A.G. EARNEST

It is a classical result, deriving from the Gaussian theory of genera of integral binary quadratic forms, that there exist only finitely many imaginary quadratic fields for which the ideal class group is a group of exponent two. This finiteness has been shown to extend to all those totally imaginary quadratic extensions of any fixed totally real algebraic number field. In this paper we put forward the conjecture that there exist only finitely many imaginary abelian algebraic number fields which have ideal class groups of exponent two, and we examine the extent to which existing methods can be brought to bear on this conjecture. One consequence of the validity of the conjecture would be a proof of the existence of finite abelian groups which do not occur as the ideal class group of any imaginary abelian field.

Introduction.

In spite of the central role in algebraic number theory played by the ideal class groups of algebraic number fields, surprisingly little is

Received 1 April 1986. This paper constitutes an expanded and updated version of a talk presented by the author at a conference at Ohio State University in June, 1982, honoring Professor Hans J. Zassenhaus.

known about the structural properties of these groups. The purpose of this paper is threefold: (1) to raise some specific questions regarding one structural invariant - the exponent - for the class groups of certain fields, (2) to survey the extent to which existing methods can be brought to bear on these questions, and (3) to analyze several well-known classes of fields.

All fields to be considered in this paper will be algebraic number fields. For such a field F, we will denote by O_F the ring of algebraic integers of F and by U_F the group of units of O_F. The class group $C_F = I_F/P_F$, where I_F is the group of all fractional ideals of F and P_F is the subgroup of principal ideals, is well-known to be a finite abelian group. The order of this group is the class number of F, which we denote by h_F. The object of study here, the exponent of the group C_F, is the smallest positive integer e for which $x^e = 1$ for all $x \in C_F$.

In the light of a classical result of Heilbronn [10], any fixed positive integer occurs at most finitely often among the class numbers of imaginary quadratic fields. In 1971 Uchida [15] proved that the finiteness of the number of fields having a fixed class number extends to the collection of all imaginary abelian fields, regardless of degree.

Employing Gauss' determination of the 2-rank of the ideal class group of a quadratic field, it follows from a theorem of Chowla [5] that there exist only finitely many imaginary quadratic fields having class groups of exponent two. This result has been generalized to the collection of all totally imaginary quadratic extensions of any fixed totally real number field [8]. In view of this generalization and Uchida's result for class numbers, it seems reasonable to ask whether this finiteness of the number of fields having class groups of exponent two can likewise be extended to a broader class of fields, perhaps to the entire collection of imaginary abelian fields. It is this question that we will address in this paper.

The results which we obtain lend support to a conjecture that there are indeed only finitely many imaginary abelian fields whose class groups

have exponent two. One interesting consequence of the truth of this conjecture would be a proof of the existence of finite abelian groups which do not occur as the class group of any imaginary abelian field.

We will treat here only the existence of fields having class groups of exponent two, although it is natural to raise the analogous finiteness questions for any fixed exponent. Such general questions appear to be intractable at this point, as even the results for the special case of imaginary quadratic fields remain incomplete.

We now give a brief outline of the contents of this paper. Known results for the exponents of the class groups of imaginary quadratic fields are surveyed in Section 1. From this point on we begin in the most general context possible and specialize further in each succeeding section. In the context of a field K which is a relative quadratic extension of a number field L, we develop in Section 2 a formula for the order of the subgroup of squares in C_K in terms of the group of units of L, the relative norm mapping from K to L, and the class groups of K and L. This formula, which is derived from a formula of Hasse and is given in Proposition 2.1, simplifies in the special case that K is a CM-field and L its maximal totally real subfield. This case is considered in Section 3. Section 4 is specialized further to imaginary abelian fields, and our most general result on the finiteness of the number of such fields having class groups of exponent two appears here as Theorem 4.2. In the final section we show how the results from the preceding sections can be applied to prove finiteness within several classes of imaginary abelian fields, including all those of degree four.

An excellent survey of the known results on class numbers of imaginary abelian fields is presented by Masley [12]. In the special case of imaginary quadratic fields there is of course a wealth of experimental evidence to draw upon when analysing class group structure. We mention here only the tables of Buell [3], which in particular indicate that certain specific small finite abelian groups (for example, the direct sum of three copies of the cyclic group of order four) do not occur as the ideal class group of any imaginary quadratic field [4]. Interesting heuristic explanations for many of the computationally observed properties of class groups, particularly in the quadratic field case, are presented in [6].

In comparison with the exponent invariant discussed here, more recent attention has been focused on other structural invariants, namely the p-ranks for various primes p, for the class groups of general number fields; see, for example, the paper of Cornell and Rosen [7].

1. Imaginary Quadratic Fields.

In this section we will survey some known results on the class groups of imaginary quadratic fields. Let $-D$ be the discriminant of an imaginary quadratic field. For convenience, in this section we will denote the class number $h_{Q(\sqrt{-D})}$ by $h(-D)$ and the exponent of $C_{Q(\sqrt{-D})}$ by $e(-D)$.

In 1934, Heilbronn [10] proved that

$$h(-D) \to \infty \quad \text{as} \quad d \to \infty . \tag{1}$$

This result can now be viewed as a direct consequence of the Siegel-Brauer theorem, which in this context asserts that

$$\frac{\log h(-D)}{\log \sqrt{D}} \to 1 \text{ as } D \to \infty . \tag{2}$$

An immediate consequence of (1) is that any fixed positive integer is the class number of at most a finite number of imaginary quadratic fields.

Also in 1934, an extension of (1) was proven by Chowla [5], who established that

$$\frac{h(-D)}{2^r} \to \infty \quad \text{as} \quad D \to \infty , \tag{3}$$

where r is the number of distinct prime divisors of D.

The significance of (3) from the present point of view arises from the fact that the 2-rank of $C_{Q(\sqrt{-D})}$ is precisely $r-1$. A generalization of (3) appears as a special case of [8; Theorem 2]. If t is any fixed positive integer and $r(t)$ denotes the 2^t-rank of $C_{Q(\sqrt{-D})}$, then that theorem implies

$$\frac{h(-D)}{2^{tr(t)}} \to \infty \quad \text{as} \quad D \to \infty . \tag{4}$$

It follows that for any fixed $t \in \mathbb{N}$, there exist at most finitely many discriminants $-D$ such that $e(-D) = 2^t$. In particular, it follows from (3) that there exist finite abelian groups which do not occur as the

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

class group of any imaginary quadratic field.

To emphasize the lack of computational effectiveness in the finiteness results for exponents, we note that in contrast to the case of class numbers, where all imaginary quadratic fields (as well as fields from some more general classes) having class number one or two have been determined (see [12] for a survey of known results), it even remains an open question whether the existing list of imaginary quadratic fields having class groups of exponent two is complete. In this regard the strongest known result is that there can exist at most one field $\mathbb{Q}(\sqrt{-D})$ with discriminant $D > 5460$ and $e(-D) = 2$ [17] .

In 1969 Iwasawa posed the problem of determining $\liminf e(-D)$ as $D \to \infty$. A conditional answer was provided by Boyd and Kisilevsky [2] in 1971 and, independently, by Weinberger [17] in 1973. Under the assumption of a suitable Generalised Riemann Hypothesis, those authors proved that

$$e(-D) \to \infty \quad \text{as} \quad D \to \infty \,. \tag{5}$$

Also contained in both of these papers is an unconditional proof that there exist only finitely many discriminants D for which $e(-D) = 3$.

2. Relative Quadratic Extensions.

The squares in the class group of $\mathbb{Q}(\sqrt{-D})$ correspond to the equivalence classes of primitive integral binary quadratic forms of discriminant $-D$ which are contained in the principal genus. Since the equivalence classes of such forms are equally distributed among all genera, and the number of such genera is 2^{r-1} , where r is the number of prime divisors of D , it follows that exactly $h(-D)/2^{r-1}$ of the elements of $C_{\mathbb{Q}(\sqrt{-D})}$ are squares. This section will be devoted to deriving the analogous formula for relative quadratic extensions.

In this section we consider number fields K and L with K a quadratic extension of L . We seek to compute the order of the subgroup C_K^2 of squares in C_K .

The primary ingredient in this computation is a formula of Hasse [9; Section 13, Satz 13] which computes the index of P_K in the subgroup $A = \{X \in I_K : X^{1-\sigma} \in P_K\}$ of I_K , where σ denotes the nontrivial

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

L-automorphism of K. Specifically,

$$[A : P_K] = h_L[N_{K/L}(\dot{K}) \cap U_L : U_L^2]2^{r-1}, \tag{6}$$

where $N_{K/L}$ denotes the relative field norm and r is the number of prime ideals of O_K which are ramified in K/L.

Consider the exact sequence $0 \to A \to I_K \xrightarrow{\phi} C_K$, where $\phi(X) = X^{1-\sigma}P_K$ for $X \in I_K$. If $G = \{X^{1-\sigma} : X \in I_K\}$, then $\mathrm{im}(\phi) = GP_K/P_K$. Thus, we have $GP_K/P_K \cong I_K/A$ and it follows that

$$|GP_K/P_K| = \frac{h_K}{[A : P_K]}. \tag{7}$$

Moreover, $C_K^2 = TP_K/P_K$, where $T = \{X^2 : X \in I_K\}$. In the familiar case where $L = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{-D})$, we have $GP_K = TP_K$ since all ideals of $O_L = \mathbf{Z}$ are principal. Hence, combining (6) and (7) yields the formula mentioned in the first paragraph of this section.

Of course O_L is generally not a principal ideal domain. So we need to consider $E = \{XO_K : X \in I_L\}$. Note that any ideal of the type $X^{1+\sigma}$, $X \in I_K$, lies in E due to the identity $X^{1+\sigma} = N(X)O_K$, where $N : I_K \to I_L$ denotes the usual norm homomorphism. It follows that $GE = TE$. So the subgroup GEP_K/P_K of C_K contains both TP_K/P_K and GP_K/P_K. The isomorphism theorems of group theory yield

$$\frac{GEP_K/P_K}{GP_K/P_K} \cong E/(E \cap GP_K)$$

and

$$\frac{GEP_K/P_K}{TP_K/P_K} \cong E/(E \cap TP_K).$$

Consequently

$$|C_K^2| = |TP_K/P_K| = \frac{|GP_K/P_K|[E : E \cap GP_K]}{[E : E \cap TP_K]}.$$

Finally, evaluating $|GP_K/P_K|$ using (6) and (7) yields:

PROPOSITION 2.1. *Let K and L be number fields with K a*

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

quadratic extension of L . *Then*

$$|C_K^2| = \frac{h_K[E : E \cap GP_K]}{h_L[N_{K/L}(\dot{K}) \cap U_L : U_L^2]2^{r-1}[E : E \cap TP_K]} \tag{8}$$

3. *CM*-Fields

We now specialize the results of the previous section to the case that K is a *CM*-field; that is, K is a totally imaginary quadratic extension of a totally real number field L . Several general relationships in this context between the class groups C_K and C_L will yield simplifications of the index factors appearing in (8).

Consider the two group homomorphisms $i : C_L \to C_K$ and $N : C_K \to C_L$, the first of which is induced by the mapping $I_L \to I_K$ given by $X \to XO_K$ and the second of which is induced by the usual norm mapping from I_K to I_L . The next proposition is a consequence of a general theorem from class field theory.

PROPOSITION 3.1. *If* K *is a CM-field with maximal totally real subfield* L , *then* $N : C_K \to C_L$ *is surjective.*

Proof. [16, Theorem 10.1].

PROPOSITION 3.2. *If* K *is a CM-field with maximal totally real subfield* L, *then the kernel of the mapping* $i : C_L \to C_K$ *has order 1 or 2* .

Proof. [16, Theorem 10.3] .

Note that the kernel of i may in fact have order two. For example, this occurs for $K = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$ which is the Hilbert class field of $L = \mathbb{Q}(\sqrt{10})$ and $(2, \sqrt{10})$ is a nonprincipal ideal of O_L which becomes principal over K .

COROLLARY 3.3. *Let* K *be a CM-field with maximal totally real subfield* L . *If* C_K *has exponent two, then*

(i) C_L *is a 2-group;*

(ii) $[E : E \cap GP_K] = 1$;

(iii) $[E : E \cap TP_K] = \lambda h_L$, *where* $\lambda = 1$ *or* $\lambda = \frac{1}{2}$.

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

Proof. (i) is immediate from Proposition 3.1. For (ii), consider $XO_K \in E$, $X \in I_L$. By 3.1, there exists $Y \in I_K$ such that $N(YP_K) = N(Y)P_L = XP_L$. Thus, $(XO_K)P_K = (N(Y)O_K)P_K = Y^{1+\sigma}P_K = Y^{1-\sigma}P_K$ since C_K has exponent two. So $E \subseteq GP_K$ as desired. Finally, for (iii), $TP_K = P_K$ implies that $[E : E \cap TP_K] = [E : E \cap P_K] = |i(C_L)|$ and the result follows from 3.2. □

From Proposition 3.1 it follows that, in the context of this section, h_L divides h_K. We denote the quotient h_K/h_L by h_K^-. In light of Corollary 3.3, equation (8) yields:

COROLLARY 3.4. *Let K be a CM-field with maximal totally real subfield L. If C_K has exponent two, then*

$$h_K^- = [N_{K/L}(\dot{K}) \cap U_L : U_L^2]2^{r-1+\mu} h_L , \tag{9}$$

where $\mu = 0$ or -1.

4. Imaginary Abelian Fields.

Finally we specialize to the case of imaginary abelian fields K; that is, for the remainder of this paper K will be a finite normal extension of $\mathbb{Q}$ having abelian Galois group and no real embeddings into $\mathbb{C}$. Such a field K necessarily has even degree $n = 2n_0$ and is a quadratic extension of its maximal totally real subfield K_0. So K is a *CM*-field and all results from the preceding section are applicable with $L = K_0$.

Uchida has proven [15] that for any positive integer N there exist only finitely many imaginary abelian fields K for which the relative class number factor h_K^- does not exceed N (somewhat more general fields are considered by Uchida, but we refer only to the abelian case here). The proof of this result consists of two major steps. First, it is shown that h_K^- becomes arbitrarily large when $\frac{n}{\log d}$ is sufficiently small, where d denotes the absolute value of the discriminant of K [15, Theorem 2]. Secondly, $\frac{n}{\log d}$ is shown to be sufficiently small for

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

almost all (not necessarily imaginary) abelian number fields [15, Proposition 1].

Minor modifications of the proof of Theorem 1 of [15] yield the following lower bound for h_K^- in terms of the discriminant d.

PROPOSITION 4.1. *For any positive number* ε, $h_K^- > d^{\frac{1}{4}-\varepsilon}$ *holds for all but finitely many imaginary abelian fields* K.

Remark 4.2. The exponent $\frac{1}{4} - \varepsilon$ appearing in the above proposition cannot be improved. To see this, consider the case that K is a cyclotomic field $\mathbb{Q}(\zeta_p)$, p prime. For such fields

$$\log h_K^- = \frac{p}{4} \log p - \frac{p}{2} \log \pi + [\tfrac{3}{4} + 7\theta] \log p ,$$

for some θ with $-1 \le \theta \le 1$ [13]. The first term on the right is $\frac{1}{4} \log d + \frac{1}{2} \log p$, so

$$\frac{\log h_K^-}{\frac{1}{4} \log d} < 1$$

for sufficiently large p.

The lower bound for h_K^- in Proposition 4.1 can be used along with equation (9) to prove the finiteness of the number of K which have class groups of exponent two and which satisfy a condition on the size of $h_0 = h_{K_0}$.

For the imaginary abelian field K, denote by h_0 and d_0 the class number and discriminant, respectively, of the maximal totally real subfield K_0. Recall that the positive integer d has the factorization

$$d = d_{K/K_0} d_0^2 ,$$

where d_{K/K_0} denotes the absolute norm of the relative different $\mathfrak{D}_{K/K_0}$ of K over K_0. For use in the proof of Theorem 4.4 we establish the following lemma.

LEMMA 4.3. *Let* ε *and* λ *be positive constants. There exist at*

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

most finitely many imaginary abelian fields K *for which*

$$d_{K/K_0}\, d_0^{\varepsilon} < \lambda^r .$$

Proof. Let p_i denote the ith rational prime and let t be the smallest positive integer for which $p_t > \lambda$. Denote $\lambda^{-t} \prod_{i=1}^{t} p_i$ by $c(\lambda)$. Observe that if $Q_1,\ldots,Q_s$ are powers of distinct prime ideals of $\mathcal{O}_K$, then $\lambda^{-s} \prod_{i=1}^{s} N(Q_i) \geq c(\lambda)^n$, where N denotes the absolute norm.

Since $\mathcal{D}_{K/K_0}$ has exactly r distinct prime factors, $\lambda^{-r} d_{K/K_0} = \lambda^{-r} N(\mathcal{D}_{K/K_0}) \geq c(\lambda)^n$. As K_0 is an abelian field, it follows from [15, Proposition 1] that there exist at most finitely many choices of K_0 for which

$$\frac{n_0}{\log d_0} \geq \frac{-\varepsilon}{2 \log c(\lambda)} .$$

So for almost all K_0, the inequality $d_{K/K_0}\, d_0^{\varepsilon} > \lambda^r$ holds for all relative quadratic extensions K of K_0.

To complete the proof it suffices to consider those K having a fixed K_0 as maximal totally real subfield. Suppose there were an infinite collection H of imaginary abelian fields K for which K_0 is the maximal totally real subfield and for which $d_{K/K_0}\, d_0^{\varepsilon} < \lambda^r$. Since only finitely many $K \in H$ have the same discriminant, d_{K/K_0} is arbitrarily large for almost all $K \in H$. Since the power to which a prime ideal divides $\mathcal{D}_{K/K_0}$ is bounded from above as a function only of n, it follows that $N(P_{K/K_0})$ is arbitrarily large for almost all $K \in H$, where P_{K/K_0} denotes the prime ideal divisor of $\mathcal{D}_{K/K_0}$ of largest absolute norm. In particular, there exist only finitely many $K \in H$ for which

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

$N(P_{K/K_0}) < \lambda c(\lambda)^{-n} d_0^{-\varepsilon}$. For all other $K \in H$ we then have $d_{K/K_0} d_0^{\varepsilon} > \lambda^r$, a contradiction. □

THEOREM 4.4. *For any positive constants* α *and* δ , *there exist at most finitely many imaginary abelian fields* K *for which* $h_0 \le \alpha d_0^{\frac{1}{2}-\delta}$ *and* C_K *has exponent two.*

Proof. Let F $(= F_{\alpha,\delta})$ denote the collection of all imaginary abelian fields for which $h_0 \le \alpha d_0^{\frac{1}{2}-\delta}$. Let F_1 and F_2 be defined as follows:

$$F_1 = \{K \in F : h_K^- \le d^{\frac{1}{4}-\frac{\delta}{8}}\}$$

and

$$F_2 = \{K \in F : 2^{n_0} > d_0^{\frac{\delta}{2}}\} .$$

Let $F' = F \setminus \{F_1 \cup F_2\}$. Since F_1 and F_2 are finite by Proposition 4.1 and [15, Proposition 1], respectively, it suffices to prove that in F' there are only finitely many fields K for which C_K has exponent two.

If K is such a field, then by equation (9)

$$h_K^- = [N_{K/K_0}(\dot{K}) \cap U_{K_0} : U_{K_0}^2]\, 2^{r-1+\mu}\, h_0 .$$

By Dirichlet's Unit Theorem, $[N_{K/K_0}(\dot{K}) \cap U_{K_0} : U_{K_0}^2] \le 2^{n_0}$. So, by definition of F' , we have

$$d^{\frac{1}{4}-\frac{\delta}{8}} < \alpha\, 2^r\, d_0^{\frac{1}{2}-\frac{\delta}{2}} .$$

Substituting $d = d_{K/K_0} d_0^2$, we have

$$d_{K/K_0}^{\frac{1}{4}-\frac{\delta}{8}}\, d_0^{\frac{1}{2}-\frac{\delta}{4}} < \alpha\, 2^r\, d_0^{\frac{1}{2}-\frac{\delta}{2}} ,$$

or

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

$$d_{K/K_0}^{\frac{1}{4}-\frac{\delta}{8}} d_0^{\frac{\delta}{4}} < \alpha 2^r .$$

But the final inequality can hold for at most finitely many imaginary abelian fields K by Lemma 4.3. □

Remark 4.5. For any $\varepsilon > 0$ and any positive integer n, the existence of infinitely many totally real fields k of degree n for which $h_k > d_k^{\frac{1}{2}-\varepsilon}$ is established in [1]. However, from the Siegel-Brauer Theorem it follows that for any $\varepsilon > 0$,

$$\frac{\log h_k R_k}{\log \sqrt{d_k}} < 1 + \varepsilon$$

holds for almost all abelian fields k, where R_k denotes the regulator of k. The regulator of any totally real field is bounded from below by $\log\left[\frac{1+\sqrt{5}}{2}\right]$ [17]. Hence, there exists a constant α_0 such that for any $\varepsilon > 0$, the inequality $h_k < \alpha_0 d_k^{\frac{1}{2}+\varepsilon}$ holds for almost all totally real abelian fields k.

5. Special types of fields.

In this section we will prove finiteness results for several specific types of imaginary abelian fields.

PROPOSITION 5.1. *There exist only finitely many imaginary normal quartic extensions K of $\mathbb{Q}$ for which C_K has exponent two.*

Proof. Let K be such a quartic field and K_0 the real quadratic subfield of K. Since C_K has exponent two, $C_{K_0}^2$ is trivial by Corollary 3.3 (i). So

$$h_0 = 2^{2\text{-rank } C_{K_0}} = 2^t ,$$

where either $t = r_0 - 1$ or $r_0 - 2$ and r_0 is the number of distinct prime divisors of d_0. So for any $\delta > 0$, $h_0 \le d_0^{\frac{1}{2}-\delta}$ holds for all

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

but at most finitely many such K_0. Since each fixed K_0 has at most finitely many imaginary quadratic extensions K for which C_K has exponent two [8, Theorem 1], the result follows from Theorem 4.4. □

In the special case that the quartic extension has noncyclic Galois group, a stronger result is readily obtained.

PROPOSITION 5.2. *Let $t \in \mathbb{N}$ be fixed. There exist at most finitely many imaginary bicyclic biquadratic fields K for which C_K has exponent 2^t.*

Proof. Let K be such a field and denote by k_1 and k_2 the imaginary quadratic subfields of K. If $X \in I_{k_i}$ $(i = 1,2)$, then $X^{2^t} O_K = (XO_K)^{2^t} \in P_K$ since C_K has exponent 2^t. Hence, $X^{2^{t+1}} = N_{K/k_i}(X^{2^t} O_K) \in P_{k_i}$. So C_{k_i} is a group of exponent 2^s, for some $0 \le s \le t+1$. It follows from (4) that there are only finitely many choices for k_i. Since k_1 and k_2 determine K, the result follows. □

PROPOSITION 5.3. *There is no prime $p \equiv 3 \pmod 4$ for which $C_{\mathbb{Q}(\zeta_p)}$ is a nontrivial 2-group.*

Proof. For $p \equiv 3 \pmod 4$, $\mathbb{Q}(\sqrt{-p})$ is a subfield of $\mathbb{Q}(\zeta_p)$ and $h_{\mathbb{Q}(\sqrt{-p})}$ is odd. If $X \in I_{\mathbb{Q}(\sqrt{-p})}$ is nonprincipal, then $XO_{\mathbb{Q}(\zeta_p)} \in I_{\mathbb{Q}(\zeta_p)}$ is nonprincipal [11; Corollary to Theorem 2]. Hence whenever $C_{\mathbb{Q}(\zeta_p)}$ is a 2-group, $h_{\mathbb{Q}(\sqrt{-p})}$ must equal one. The only primes $p \equiv 3 \pmod 4$ for which $h_{\mathbb{Q}(\sqrt{-p})} = 1$ are $p = 3,7,11,19,43,67$ and 163. $h_{\mathbb{Q}(\zeta_p)} = 1$ for the first four of these values of p, $h_{\mathbb{Q}(\zeta_{43})} = 211$, and $h_{\mathbb{Q}(\zeta_{67})} = (67)(12739)$ (see [16]). The smallest odd prime divisor of the first factor of $h_{\mathbb{Q}(\zeta_{163})}$ is 181 (see [16]). □

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press

Remarks 5.4. (1) If $m|n$, then $h_{\mathbb{Q}(\zeta_m)} \Big| h_{\mathbb{Q}(\zeta_n)}$. So $h_{\mathbb{Q}(\zeta_n)}$ has an odd prime factor whenever n has an odd prime factor $p \equiv 3 \pmod 4$, $p \neq 3,7,11,19$.

(2) The only prime p for which $C_{\mathbb{Q}(\zeta_p)}$ is a 2-group and $h_{\mathbb{Q}(\zeta_p)} < 10^6$ is $p = 29$, for which the class group is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The only composite values of m for which $C_{\mathbb{Q}(\zeta_m)}$ is a 2-group and $h_{\mathbb{Q}(\zeta_m)} < 10^6$ are $m = 39,56,65,68$ and 120, for which the class numbers are $2,2,64,8$ and 4, respectively. Of these, $C_{\mathbb{Q}(\zeta_{68})}$ and $C_{\mathbb{Q}(\zeta_{120})}$ are cyclic; the structure of $C_{\mathbb{Q}(\zeta_{65})}$ has not been determined. These numerical results are extracted from [12] and [14].

References

[1] N.C. Ankeny, R. Brauer and S. Chowla, "A note on the class numbers of algebraic number fields", *Amer. J. Math.* 78 (1956), 51-61.

[2] D.W. Boyd and H. Kisilevsky, "On the exponent of the ideal class group of complex quadratic fields", *Proc. Amer. Math. Soc.* 31 (1971), 433-436.

[3] D.A. Buell, "Class groups of quadratic fields", *Math. Comp.* 30 (1976), 610-623.

[4] D.A. Buell, "Small class numbers and extreme values of L-functions of quadratic fields", *Math. Comp.* 31 (1977), 786-796.

[5] S. Chowla, "An extension of Heilbronn's class number theorem", *Quart. J. Math., Oxford Ser.* (2) 5 (1934), 304-307.

[6] H. Cohen and H.W. Lenstra, Jr., "Heuristics on class groups of number fields", *Number Theory Noordwijkerhout 1983*, pp. 33-62. (Springer-Verlag, Berlin-Heidelberg-New York-Tokyo 1984).

[7] G. Cornell and M. Rosen, "Group-theoretic constraints on the structure of the class group", *J. Number Theory* 13 (1981), 1-11.

[8] A.G. Earnest and O.H. Körner, "On ideal class groups of 2-power exponent", *Proc. Amer. Math. Soc.* 86 (1982), 196-198.

[9] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörpern*, Teil I, Ia, 2 Aufl., Würzburg-Wien, 1965.

[10] H. Heilbronn, "On the class-number in imaginary quadratic fields", *Quart. J. Math., Oxford Ser.* (2) 5 (1934), 150-160.

[11] Y. Kitaoka, "Scalar extension of quadratic lattices", *Nagoya Math. J.* 66 (1977), 139-149.

[12] J.M. Masley, "Class groups of abelian number fields", *Queen's Papers in Pure and Appl. Math.* 54 (1980), 475-497.

[13] J.M. Masley and H.L. Montgomery, "Unique factorization in cyclotomic fields", *J. Reine Angew. Math.* 286/287 (1976), 248-256.

[14] K. Tateyama, "On the ideal class groups of some cyclotomic fields", *Proc. Japan Acad., Ser. A Math. Sci.* 58 (1982), 333-335.

[15] K. Uchida, "Class numbers of imaginary abelian number fields, I", *Tôhoku Math. J.* 23 (1971), 97-104.

[16] L.C. Washington, *Introduction to Cyclotomic Fields*, (Springer-Verlag, New York-Heidelberg-Berlin, 1982).

[17] P. Weinberger, "Exponents of the class groups of complex quadratic fields", *Acta Arith.* 22 (1973), 117-124.

[18] R. Zimmert, "Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung", *Invent. Math.* 62 (1981), 367-380.

Department of Mathematics
Southern Illinois University
Carbondale
Illinois 62901.
United States of America.

Notes Added In Proof.

(1) In equation (6), $r = r_0 - r_1 - r_2 + u$, where r_0 is the number of prime ideals of O_L which are ramified in K/L, r_1 and r_2 are the numbers of real and complex archimedean prime spots on L, respectively, and u is the number of real archimedean prime spots on L over which there lies a complex archimedean prime spot on K.

(2) Professor Kitaoka has kindly pointed out that the reference [11] does not suffice on p.243; the appropriate reference here is to Corollary 2 of

R. Gold and P. Ponomarev, *Scalar extensions of binary lattices*, Number Theory and Algebra (Academic Press, 1977), 91-95.

https://doi.org/10.1017/S0004972700013198 Published online by Cambridge University Press